The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/05/2017

SUBJECT:
A Vulnerability in WordPress Content Management System Could Allow for Security Bypass

OVERVIEW:
A vulnerability has been discovered in WordPress content management system (CMS), which could allow for security bypass. WordPress is an open source content management system for websites. Successful exploitation of this vulnerability could allow for attackers to reset an administrative password for a website running the affected versions of WordPress.

THREAT INTELLIGENCE
While a proof of concept is available, there are no reports of this vulnerability being actively exploited in the wild at this time.

SYSTEM AFFECTED:
- WordPress versions 4.7.4 and earlier

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in WordPress which could result in the unauthorized reset of an administrative account. This vulnerability exists because WordPress relies on the host HTTP header for a password reset email and fails to properly validate the server name. An attacker can exploit this issue by modifying the host name in a specifically crafted HTTP POST to the affected website. This will cause the password reset email to be sent to an attacker controlled email address, allowing the attacker access to the password reset link. While the owner of the targeted account will also receive the reset email, providing indication of a potential compromise, the attacker will gain access for an indeterminate length of time. (CVE-2017-8295)

Successful exploitation of this vulnerability could allow for attackers to reset an administrative password for a website running WordPress.

RECOMMENDATIONS:
The following actions should be taken:

- Ensure no unauthorized systems changes have occurred before applying patches.
- Update WordPress CMS to the latest version once a patch has been released after appropriate testing.
- Review and follow WordPress hardening guidelines - http://codex.wordpress.org/Hardening_WordPress.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295

Exploit-DB:
https://www.exploit-db.com/exploits/41963/